Press Release

Amicus ITS Awarded Full Certification For Cyber Essentials Plus

Standards Co-Ordinator Emma Purr with System Administrator Rob Crespin

3rd March 2017

Amicus ITS has announced it has been awarded higher level 'Cyber Essentials Plus' status. This industry-backed technical security scheme seeks to heighten the defences of companies against threat. For Amicus ITS with its long history of serving healthcare, regulated industries and blue chip corporates, it was a logical and natural extension of its existing security standards.

The security project which started in September 2016, was led by Standards Co-Ordinator **Emma Purr** of Amicus ITS' Security & Compliance Team, supported by members of the Amicus ITS technical Escalation Team.

Commenting on the award, **Emma Purr** said: *"Cyber Essentials Plus is normally a first step-in for organisations to gain the more stringent security accreditation, ISO 27001. Cyber Essentials Plus requires a 5 step security approach, whilst information security standard ISO27001 has 114 control requirements in 14 groups and 35 control objectives which must be addressed. However, we've done it in reverse, having gained our ISO27001 status back in July 2014. This was however no walk in the park and illustrates the critical importance of ensuring robust defences exist around your business. Obtaining Cyber Essentials Plus status has further strengthened our resilience and is great to have on show as another recognised security badge.*

JP Norman, Director of Technology, Security & Governance added: *"I am very proud of the collective effort everyone made to helping us achieve this certification. It perfectly demonstrates that even amongst very competent teams, there is always an opportunity to increase awareness throughout the business, which not only supports Amicus ITS, but all our customers' data and systems too".*

Anyone wishing to discuss business information security issues or about being supported to obtain Cyber Essentials status, should contact the Sales team on 02380 429429.

What is Cyber Essentials Plus about?

To create the UK Cyber Essentials scheme, the UK Government worked with the Information Assurance for Small and Medium Enterprises (IASME) consortium and the Information Security Forum (ISF) for several years before launching the current system in June 2014. Backers also include the Federation of Small Businesses (FSB), the Confederation of British Industry (CBI)

and various insurance institutions. Forming a set of comprehensive and challenging technical controls, it endorses compliance for organisations to create better technical protection from cyber attack and misuse of systems. With standards which are risk-based and prompted by international best practice, they include aspects such as physical security, staff awareness and data backup.

What does Cyber Essentials Plus focus on?

Amicus ITS had to focus on 5 mitigation strategies:

1. Boundary firewalls and internet gateways – for any user trying to access any websites which may have malicious content
2. Secure configuration – ensuring the administration control of all user devices are securely configured, so the rights on what can be downloaded is appropriate and controlled.
3. User access control eg, new starters only have access to the systems they require as part of their job; special access privileges which are restricted to a limited number of authorised individuals, which includes domain admin and the restriction of selected system administrators to be able to make any changes at a high level to internal systems and security firewalls; plus password strengthening and complexity in relation to service accounts. These get changed regularly - and automatically on the exit of any personnel.
4. Malware protection – ensuring that relevant antivirus malware software is installed and kept up to date, which scans files and web locations automatically on access to identify they are safe and also to reindorse the protection against accessing unsafe websites which get automatically blocked.
5. Patch management – this ensures all software running on company devices are licenced and up to date, installed in a timely manner and that out of date software is removed from devices. Additionally, that security patches are deployed automatically on release.